⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭63－229541

⑤1Int.Cl.⁴	識別記号	庁内整理番号	④3公開　昭和63年(1988)9月26日
G 06 F 12/14	310	C－7737－5B	

審査請求　有　請求項の数 5　（全4頁）

⑤4発明の名称　データ交換システム

⑳特　願　昭63－47338

㉒出　願　昭63(1988)2月29日

優先権主張　㉜1987年3月4日㉝西ドイツ(DE)㉛P3706957.8

⑦2発明者　ディートリツヒ、クルーゼ　ドイツ連邦共和国オツトーブルン、ウルメンシユトラーセ9

⑦2発明者　アルブレヒト、ボイテルシユパツヒアー　ドイツ連邦共和国オツトーブルン、シユワルベンシユトラーセ78

⑦2発明者　アネツテガブリエル、ケルステン　ドイツ連邦共和国ウイースバーデン、フラウエンロープシユトラーセ6

⑦1出願人　シーメンス、アクチエンゲルシヤフト　ドイツ連邦共和国ベルリン及ミユンヘン（番地なし）

⑦4代理人　弁理士　富村　潔

明　細　書

1．発明の名称　データ交換システム

2．特許請求の範囲

1）少なくとも1つのデータ入力／データ出力装置とチープカードの形態の少なくとも1つの携帯可能なデータ担体とを有するデータ交換システムであって、データ入力／データ出力装置およびチープカードがそれぞれ付属の制御およびアドレス指定回路を有する独立したプログラム可能なデータメモリと、それぞれマイクロプロセッサのなかに組み込まれている共通の真正確認アルゴリズムと、記憶されたそれぞれ等しい秘密キーとを備えているデータ交換システムにおいて、カストマーカード（KK）としての役割をするチープカードが乱数発生器を含んでおり、その都度発生された乱数（v）がカストマーカード（KK）のなかでもカストマー端末器（KT）としての役割をするデータ入力／データ出力装置のなかに伝達後にもデータメモリからプログラム（P）の一部をデータフロー制御のために選択し、これらのプログラム部分（Pv）から真正確認アルゴリズム（f）および秘密キー（KPC）を利用してそれぞれ真正確認コード（PACv）が計算され、またカストマーカード（KK）のなかに比較装置（COMP）が設けられ、この比較装置が一方ではカストマーカード（KK）のなかで計算された真正確認コード（PACv）および他方ではカストマー端末器（KT）のなかで計算されかつカストマーカード（KK）のなかに伝達された真正確認コード（PACv）の同一性を検査することを特徴とするデータ交換システム。

2）カストマー端末器（KT）のなかで選択されたプログラム部分（Pv）が固有の安全モジュールのなかに伝達され、そのなかで真正確認コード（PACv）がそこに格納されている秘密コード（KPCs）およびそこに組み込まれている真正確認アルゴリズム（fs）

を利用して計算され、また計算された結果が直接にカストマーカード（ＫＫ）のなかの比較装置（ＣＯＰＭ）に伝達されることを特徴とする請求項１記載のデータ交換システム。

3) 安全モジュールが差し込みカード（ＳＫ）として構成されていることを特徴とする請求項１記載のデータ交換システム。

4) データフロー制御のためのプログラム（Ｐ）からのデータ（Ｐｖ）の選択が、各第ｋビットまたはバイトが選択されるように行われることを特徴とする請求項１ないし３の１つに記載のデータ交換システム。

5) プログラムデータ（Ｐｖ）の選択が、第１の乱数発生器の出力信号により始動される第２の乱数発生器により制御されることを特徴とする請求項１ないし３の１つに記載のデータ交換システム。

３．発明の詳細な説明

〔産業上の利用分野〕

この発明は、少なくとも１つのデータ入力／データ出力装置とチープカードの形態の少なくとも１つの携帯可能なデータ担体とを有するデータ交換システムであって、データ入力／データ出力装置およびチープカードがそれぞれ付属の制御およびアドレス指定回路を有する独立したプログラム可能なデータメモリと、それぞれマイクロプロセッサのなかに組み込まれている共通の真正確認アルゴリズムと、記憶されたそれぞれ等しい秘密キーとを備えているデータ交換システムに関するものである。

〔従来の技術〕

最近のデータ処理および通信システムではデータの保護がますます重要な役割を演ずる。システムがデータ保護に関し十分な対策を施しているかどうかは、システムへのアクセスを正当な人に対してのみ可能にし、逆に不当な人を絶対的な安全性をもって締め出すことがどの程度に達成されているかどうかに決定的に関係する。システムへのアクセスの正当性を検査するための絶対的に安全ではないが簡単な方法は、たとえば、正当な利用者にのみ知られており、また利用者により任意に頻繁に変更できるいわゆるパスワードを使用する方法である。パスワードは、無資格者により探知または盗聴される危険があるので、補助的な安全対策が不可欠である。これらの対策の一つは、たとえば、伝達される情報の暗号化およびその解読であり、データ処理システムにおいてなかんずくチップカードの利用によっても実現可能である対策である。

データ処理システムにチップカードがますます取り入れられると、他方において、チップカードは比較的紛失しやすいので、再び安全性に関して別の危険が生ずる。従って、チップカードが紛失の際にあらゆる場合に不正使用に対して保護できるように配慮されることが不可欠である。従ってチップカードは、予めチップカードのなかにのみ記憶されている識別子、たとえば個人識別番号、いわゆるＰＩＮが利用者により入力される時にのみ、保護されたチップカードのなかに記憶されているデータにアクセス可能となるように構成されている。

別の安全対策手段はシステムに対するチップカードの真正確認を利用して構成され得る。この真正確認は、任意の加入者が正当であると虚偽の申し立てをすることによりシステム内の秘密情報にアクセスすることを防止する。真正確認のための重要な前提は加入者の個人別のコピー不可能な特徴である。加入者のこのコピー不可能な特徴は、両パートナー（すなわちチップカードとシステムの両者）に、一層詳細にはこれらの両パートナーにのみ知られている暗号化およびその解読のための秘密のキーを利用することにより得られる。

しかしながら、チップカードと利用者端末器との間の緊密な回路技術的結び付きは、チップカードの利用者のみがそのアイデンティティを証明するだけでなく、端末器の側でもデータフローが端末器内で操作されずに進行することが保証されていることをも前提とする。その例は、チップカード利用者により書込まれた識別番号ＰＩＮが読出され得ないこと、また端末器により指示されたデ

ータがチップカードに伝達されたデータに一致することである。従って、利用者に真正らしいデータが指示されたり、またチップカード内で誤ったデータが処理されるような操作は絶対的な安全性をもって排除されなければならない。

〔発明が解決しようとする課題〕

本発明の課題は、冒頭に記載した種類のデータ交換システムを、利用者端末器内の操作不可能なデータフロー制御が保証されるように構成することである。

〔課題を解決するための手段〕

この課題は、本発明によれば、カストマーカードとしての役割をするチープカードが乱数発生器を含んでおり、その都度発生された乱数がカストマーカードのなかでもカストマー端末器としての役割をするデータ入力／データ出力装置のなかに伝達後にもデータメモリからプログラムの一部をデータフロー制御のために選択し、これらのプログラム部分から真正確認アルゴリズムおよび秘密キーを利用してそれぞれ真正確認コードが計算され、またカストマーカードのなかに比較装置が設けられ、この比較装置が一方ではカストマーカードのなかで計算された真正確認コードおよび他方ではカストマー端末器のなかで計算されかつカストマーカードのなかに伝達された真正確認コードの同一性を検査することにより解決される。本発明の有利な実施態様は請求項2以下にあげられている。

〔実施例〕

以下、本発明の実施例を図面により一層詳細に説明する。

第1図には、左部にチップカードとして構成されたカストマーカードＫＫが、また右部にいわゆるカストマー端末器ＫＴが示されており、それらのなかに本発明にとって主要な回路要素が形成されている。カストマー端末器ＫＴのなかにデータフロー制御のための正しいプログラムＰが存在しているか否かは、個人識別番号ＰＩＮの入力前にカストマーカードＫＫにより、もしくはたとえば毎日の作業開始時に検査用チップカードにより検査される。この検査はクリプトグラフィックな方法により行われる。そのために、カストマー端末器ＫＴのメモリのなかに格納されている外部に対し秘密にすべきプログラム部分Ｐが個人化の際にカストマーカードまたは検査用カードのなかに参照データとして記憶されることが必要である。さらに、カストマー端末器ＫＴにおける秘密キーＫＰＣの確実な記憶が可能であることが前提とされている。さらに、カストマーカードＫＫおよびカストマー端末器ＫＴの両者に共通の真正確認アルゴリズムｆをが与えられている。この真正確認アルゴリズムｆおよび秘密キーＫＰＣを利用してプログラムデータからカストマー端末器ＫＴおよびカストマーカードＫＫの両者において真正確認パラメータまたはプログラム真正確認コードＰＡＣｖが計算される。偽造されたプログラムにもかかわらずプログラム真正確認コードＰＡＣｖのコピーによる盗聴アクセスおよび操作を予防するため、乱数ｖを利用してダイナミックなプログラム検査が行われる。乱数ｖはカストマーカードＫＫのなかで発生され、さらにカストマー端末器ＫＴに伝達される。これにより乱数ｖに関係して、カストマーカードＫＫのなかでもカストマー端末器ＫＴのなかでも秘密なプログラム部分Ｐからデータブロック Ｐｖが選択される（モジュールＳＥＬを参照）。従って、プログラム・真正確認コードＰＡＣｖの前記の計算はこの選択されたデータブロックＰｖに基づいて関係式

$$PACv = f(KPC; Pv)$$

に従って行われる。計算された両プログラム・真正確認コードＰＡＣｖの一方、詳細にはカストマー端末器ＫＴのなかで計算されたプログラム・真正確認コードが最終的にカストマーカードＫＫに伝達され、そこでそこに設けられている比較装置ＣＯＭＰが、カストマーカードＫＫにより計算された結果とカストマー端末器ＫＴにより計算された結果とが一致するか否かを確認する。

カストマーカードＫＫのなかにもカストマー端末器ＫＴのなかにも格納される秘密キーＫＰＣの確実な記憶のためには2つの方法がある。第1の

方法は、秘密キーＫＰＣを確実なプログラム可能な読出しメモリのなかに格納する方法である。第２の方法では、キーＫＰＣが特殊なチップカードからカストマー端末器ＫＴのカード読取り装置を介してカストマー端末器の書込み・読出しメモリのなかに読込まれる。このメモリに対する電流供給は外部から行われる。

真正確認アルゴリズムｆとしてワンウェイ・ファンクションが使用されると好適である。このアルゴリズムは、比較的容易にチップカードのなかに組み込まれるように、複雑さの少ないものでなければならない。

乱数ｖを利用して秘密プログラム部分Ｐからデータブロック Ｐｖを選択するためには多くの方法が考えられる。たとえば各第ｋビット／バイトがプログラム部分Ｐから選択されればよく、その際ｋは固定であり、また選択により開始されるべき乱数ｖを決定する。またはｋ＝ｖであり、また開始はプログラム部分Ｐの第１のビット／バイトで行われる。しかし、乱数ｖはたとえば出発値として別の乱数発生器を始動させ、その出力信号が選択されたデータブロックＰｖに対するビット／バイトを決定してもよい。

チップカードＫＫのなかに秘密プログラム部分に対して過大なメモリ容量を必要としないように、記憶されたプログラム部分Ｐはカード固有であってもよい。それにもかかわらずカードの全体により、すべての秘密プログラム部分Ｐの検査が保証される。

端末器のなかに相異なるカードシステムを使用する際には、プログラム・真正確認コードＰＡＣｖがカストマー端末器ＫＴではなく固有の安全モジュールにおいて、たとえば取扱者端末器における固有の安全カードＳＫ（第２図参照）において検査されることによって、プログラム検査はシステムに無関係に行われ得る。カード提示者に、プログラム検査を行うべきか否か、またその仕方が任されている。特に、真正確認アルゴリズムｆｓおよび秘密キーＫＰＣｓは提示者により自由に選択可能である。この形態のプログラム検査の別の利点は、秘密キーがカストマー端末器ＫＴ内には記憶される必要がないことである。

４．図面の簡単な説明

第１図は本発明によるデータ交換システムにおけるデータフローを検査するための回路装置のブロック図、第２図は第１図による回路装置の変形例のブロック図である。

ＫＫ…カストマーカード

ＫＴ…カストマー端末器

Ｐ…外部に秘密にすべきプログラム部分

ＫＰＣ…秘密キー

ｆ…真正確認アルゴリズム

ＰＡＣ…プログラム・真正確認データ

ｖ…乱数

Ｐｖ…選択されたデータブロック・プログラム部分

ＳＥＬ…選択モジュール

ＣＯＭＰ…比較装置

Ｓｋ…安全カード

ｆｓ…Ｓｋ内の真正確認アルゴリズム

FIG 1

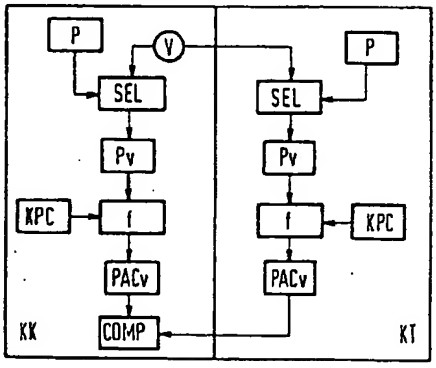
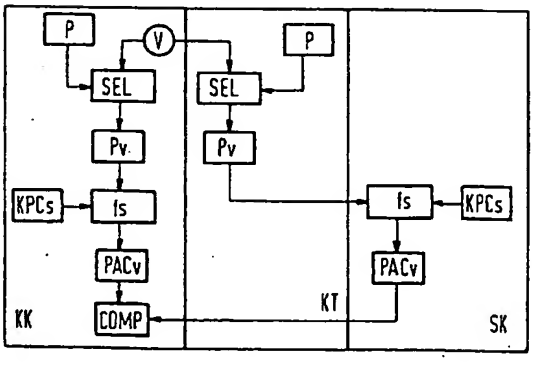


FIG 2



(8118) 代理人 弁理士 富村